PATENT
Attorney Docket No. P1907US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Girault et al.

Application No. 10/519,698

Art Unit: 2431

Examiner: Sarah Su

Filed: December 27, 2004

For: CRYPTOGRAPHIC METHOD AND DEVICES FOR FACILITATING CALCULATIONS DURING TRANSACTIONS

REQUEST FOR PRE-APPEAL BRIEF CONFERENCE

Mail Stop AF
Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

The Applicants respectfully request a pre-appeal brief conference pursuant to the U.S.P.T.O. Official Gazette Notice "New Pre-Appeal Brief Conference Pilot Program" dated 12 July 2005, as extended by the U.S.P.T.O. Official Gazette Notice "Extension of the Pilot Pre-Appeal Brief Conference Program" dated 07 February 2006. As required by this procedure, Applicants are herewith providing, in five or less total pages, a succinct, concise and focused set of arguments for which the review is being requested. Page references used herein refer to the Final Office Action of November 18, 2009, unless otherwise indicated. Paragraph numbers referring to the specification are to the published application.

Applicants sincerely thank the Examiner for her efforts in conducting the telephone interview on January 21, 2010, and helpful comments made therein. Applicants further emphasize that the filing of this Notice of Appeal does not suggest an end to the willingness of Applicants to further work with the Examiner in developing patentable subject matter in this application. Applicants welcome any suggestions or comments that might help achieve the proper scope of claims. As requested by the Examiner in the Interview Summary, mailed January 27, 2010, Applicants have herein attempted to further clarify the differences between the claimed invention and RSA digital signal authentication.

CONCISE AND FOCUSED SET OF ARGUMENTS ON FIVE PAGES OR LESS

BACKGROUND

Claim 1 is exemplary of the scope of protection sought in the application, and therefore this claim is the focus of this request.

In simplified form, claim 1 is directed to a cryptographic method for authenticating a transmitted message using RSA public-private key cryptographic techniques. In the prior art, which includes standard RSA authentication techniques, a sender (or "prover") can send a message along with a digital signature authenticating the message. As noted in ¶ [0015], the RSA algorithm has a problem because of the large number of operations that must be carried out by the prover or the signer—to the extent that dedicated cryptographic hardware must be used in order to achieve reasonable calculation times (particularly in certain time-sensitive contexts, like e-commerce). Since such hardware can significantly increase costs, it is desirable to eliminate such hardware, while at the same time permitting rapid signature/authenticating calculations to take place.

The subject matter of claim 1 achieves this by splitting the operation-intensive calculations and resultant elements of proof into two parts: the first part is one that can be done in advance, e.g., of a transaction, and the second part is one that can be done rather quickly. These are referred to in the claims as, respectively, the first element of proof, and the second element of proof, and would be generated by the prover who bears the burden of proving authenticity. The calculations specified in claim 1 make the method compatible with the use of RSA keys, while at the same time not sacrificing the level of security afforded in the known RSA scheme.

Final Office Action

The Examiner rejected claim 1 as being obvious over **Rivest**, et al. ("A Method for Obtaining Digital Signatures and Public-Key Cryptosystems") in view of **M'Raihi** (U.S. Patent No. 5,946,397).

EXAMINER'S POSITION

Rivest—With regard to Rivest's teaching, the Examiner stated, on p. 4 that Rivest discloses:

> generating, at the first entity, a first element of proof (i.e. E) by using a generic number (i.e. M) raised to a first power, modulo the modulus (i.e. n), having a first exponent equal to the public key exponent (i.e. e) multiplied by a random integer (i.e. d) kept secret by the first entity, whereby calculation of said first element of proof is executable independently of the transaction (paragraph 5, line 16; paragraph 6, line 22);

> generating, at the first entity, a second element of proof (i.e. public key) related to the first element of proof and dependent on a common number (i.e. n) shared by the first and second entities specifically for the transaction (paragraph 5, lines 31-47).

In responding to Applicants' arguments, the Examiner stated (p. 2):

> Rivest discloses that E is calculated by raising M (i.e. generic number) to a power equal to the public key exponent (i.e. e) multiplied by a random integer (i.e. d), modulo the modulus (i.e. n) (paragraph 5, line 16; paragraph 6, line 22).
>
> Rivest discloses that the integer d is picked to be a large, random integer (paragraph 5, lines 39-40).

M'Raihi—The Examiner acknowledged that Rivest fails to teach or suggest the last claimed element, the verifying step, but then provided the M'Raihi reference as filling this missing teaching. The Examiner stated, on p. 5, that M'Raihi discloses:

> verifying, at the second entity that the first element of proof (i.e. x) is related through a relationship with a second power, modulo the modulus, (i.e. p) of a generic number (i.e. g) having a second exponent (i.e. k) equal to a linear combination of at least part of the common number and of the public key exponent multiplied by the second element of proof (col. 2, lines 44-49).

The Examiner countered Applicants arguments in the Response to Arguments section on p. 3, stating:

> It is argued by the applicant that M'Raihi does not disclose verifying the relationship between $x = g^{ey+e}$, where the linear combination uses a public key exponent multiplied by the second element of proof. The examiner respectfully disagrees. M'Raihi discloses that a g (i.e. a generic number) is raised to the power k, which is a linear combination of the base (i.e. common number) (col. 4, lines 31-41), which is made up of (x_i, z_i), where x is the key and x_i is the public key exponent (col. 2, lines 40-42; col. 3, lines 45-46). M'Raihi also discloses that the exponents x_i could be loaded beforehand into a reprogrammable memory by the authority (col. 3, lines 40-46).

APPLICANT'S POSITION

An element of proof is a value that is easily created by a prover (authenticator), impossible to create by an imposter (anyone other than the prover), but easily verifiable by a verifier—Rivest deals with elements that apply to encryption and decryption, not authentication/signature proof despite certain related mathematical equations.

Applicants respectfully disagree with the Examiner's characterization of the teaching of both Rivest and M'Raihi. First, Applicants consider the term "element of proof" as would be understood by

one of ordinary skill in the cryptographic arts. An "element of proof" is some form of evidence offered by a prover to prove, in some way, that the prover, and only the prover (to be effective), could possess such evidence. In the RSA system, this is some number that is determinable only by one who possesses certain secret information (the private key). Although an imposter would find it impossible to *create* such an element of proof, the element of proof can be relatively easily *verified* by others. Thus the "element of proof" is a numerical value that is easy for the prover to create, but impossible for anyone else to create, but is easy to verify by others.

The mathematical calculations in both Rivest and M'Raihi bear some resemblance to those in claim 1—this is of necessity since all of these deal with RSA-related algorithms, and one of the stated goals of the invention is that it maintains compatibility with the use of RSA public and private keys. Therefore, there would clearly need to be some overlap of the low-level equations. However, there are fundamental differences in how these are applied at a higher and practical level.

Rivest discusses a method for encrypting and decrypting messages and not one of authentication. The Examiner equates Rivest's element E as disclosing the claimed first element of proof. However, Rivest's E is not the same thing as an element of proof and differs in some fundamental ways. Most importantly, Rivest's E is not used to *prove* anything—it is an encryption procedure. As such, it is an algorithm that is used to create ciphertext C... it is not an integer, as the first element of proof must be in order to meet the other elements of claim 1, and one of ordinary skill in the art to equate an algorithm with an integer (Rivest, p. 120, (II) ¶1). Second, the first element of proof, by its nature, is one that only an authenticator can create. If anyone (e.g., an imposter) could create a value that is the same as the first element of proof, this value could not be used to prove authentication. Rivest's E (the encryption procedure), in contrast, is publicly available and can be used by anyone to encrypt the message. Thus, *anyone* can create E (using the recipients public procedure/key). Clearly, the first element of proof and the encryption procedure E represent two very different things and are used in two very different ways, despite surface similarities in the low-level mathematics involved.

Furthermore, in Rivest § V, line 16, "E" is defined with the equation $E(M)=M^e$ which does *not* involve the integer d (which the Examiner indicated is equated to the random integer used to calculate the first element of proof). Although in Rivest § VI, line 22, the equation $E(D(M))=M^{e*d}$ is disclosed, this is used to show the relationship between the encryption procedure E and the decryption procedure D, i.e., it illustrates that a properly encrypted message can be decrypted with the right information. Such an equation is shown in Rivest simply to prove that, mathematically speaking, algorithms E and D are permutations (§ VI is about "the Underlying Mathematics"). § VI does not disclose that the value

E(D(M)) is actually generated or calculated, nor would one have any reason to do so. Additionally, in Rivest, algorithm E is to be carried out in a *first encrypting* entity (Bob for instance), whereas the algorithm D is to be carried out in a *second decrypting* entity (Alice for instance). Therefore, the calculation of M^{e*d} in Rivest, as shown in § VI, line 22, implies two different entities. In distinct contrast, the first generation step of claim 1 occurs in a *single* first entity.

Moreover, Rivest fails to disclose the second step of generating, at *the first entity,* a second element of proof related to the first element of proof and dependent on a common number shared by the first and second entities specifically for the transaction. The Examiner indicated that the encryption public key (e,n) in Rivest would disclose this feature. More precisely, the positive integer n would be the common number shared by the first and second entities on which the second element of proof would be depending. However, Rivest fails to disclose explicitly that such a second element of proof is actually generated *at the first entity* (in other words, in the same entity where the first element of proof is generated). Claim 1 requires that both the first and second element of proof are calculated by the same entity—as would make sense to have the prover generate the necessary two pieces of authenticating proof. In the Response to Arguments section, the Examiner indicated that a sender encrypting a message (with the pair (e,n)) would need to generate a public encryption key in order to encrypt the message. However, Applicants respectfully assert that this assumption is correct for the following reason.

The pair (e,n) is a *public* encryption key and does not necessarily need to be generated in the first entity using it for encryption. Furthermore, in Rivest § V, lines 30-51, the successive steps of computing n, d and e are disclosed. In particular, e is generated from integer d, which is part of a *private* decryption key kept secret in the second entity (see lines 44–47). From this passage, it appears that, in order to keep the secrecy of integer d, the generation of e should occur in the *second* decrypting entity, and not in the *first* encrypting entity. Therefore, one cannot find a teaching in Rivest that the generation of a second element proof equating to integer e must happen in the first entity.

M'Raihi does not disclose the verifying relationship $x=g^{ey+c}$, as required by claim 1— The Examiner provided the M'Raihi reference as completing the disclosure for the third claimed element missing from the disclosure of Rivest, indicating that M'Raihi discloses that a signature element r is generated according to $r=g^k$, where "k is a linear combination of the base (col. 4, lines 31–41) which is made up of (x_i,z_i) where x is the key and x_i is the public key exponent".

Applicants cannot find these elements in the cited passages. The numbers x_i used in the database are random numbers (col. 4, lines 8–11) rather than the public key exponent. The number x is the secret key (col. 3, lines 45–46) but does not appear in the calculation to obtain k. Public key y (col.

3, lines 45–46) is neither used in the computation of the exponent k.

The value k in M'Raihi results from the linear combination of the multiplied random variables a_i and x_i and does not appear to be related in any way with a common number shared by both entities El and E2, as it is the case in claim 1.

Moreover, M'Raihi fails to disclose that the linear combination uses a public key exponent *multiplied* by the second element of proof. As already mentioned, the exponent k results from a linear combination of x_i values, this is to say to a sum of a_i*x_i (see col. 4, line 35) where a_i and x_i are random numbers (col. 4, lines 9–10 and 28–30). Since these number are clearly stated as being *random*, they cannot be considered either as a public key exponent or as a second element of proof, for instance, in the sense of the element E in Rivest.

Standard RSA authentication scheme differs from the claimed authentication in that standard RSA authentication does not utilize both first (harder to calculate and calculable independently of the transaction) and second elements of proof (easier to calculate). The standard RSA authentication scheme (see para. [0010]–[0015] has the prover A calculating a single value W' that serves as the authenticating value (or, perhaps, "*sole* element of proof"), since this value is impossible to forge by an imposter. One main goal of the present invention is to split the element of proof into two separate elements of proof: a first element of proof (x), and a second element of proof (y) that are related to one another. The first element of proof requires somewhat laborious calculations, and this can be calculated independently of the transaction (para. [0022]), and the second element of proof can be calculated fairly quickly, thereby saving time at the actual point of the transaction.

Respectfully submitted,

/brian c. rupp/

Brian C. Rupp, Reg. No. 35,665
Mark Bergner, Reg. No. 45,877
DRINKER BIDDLE & REATH LLP
191 N. Wacker Drive, Suite 3700
Chicago, Illinois 60606-1698
(312) 569-1000 (telephone)
(312) 569-3000 (facsimile)
Customer No. 08968

Date: February 16, 2010